Week 2

Actors

- Hackers → to get privileged info
- Internal users → installation of malware
- Hacktivism → similar to governments; carry out DDOS attack.
- Governments → spy & monitor important politicians via APT.

Motivation Factors.

1.) Just play (Fun)
2.) Gain Money
3.) Political Action and movements
4.) Hire me!

Hacking Organization.

→ Fancy Bears'

Major different types of Cyber Attacks.

Sony Hack - 2011
Singapore Cyber Attacks 2013
Target - 2015 100 million Credit cards were leaked.

and etc.

Emerging Cyber Attacks → Banks.
VISA / Mastercard
Identification problems.

Tools & Attacks used Regularly.

1.) Wannacry (North Korea)
2.) Darkseoul
3.) Duqu and Flame (Olympic Games)
4.) Shamoon (Iran)
5.) Black Energy 3.0 (Russia)
6.) SeaDaddy and seaDuke (USElecti

An Architects perspective on attack Classification.

Security Attack Classification.

Passive Attacks → eavesdropping style of attacks

→ Second class is traffic analysis

Active Attacks. → explicit interception and modification
→ several classes of these attacks exist.

→ Masquerade
→ Replay
→ Modification
→ DOS

Security Services
→ A processing or communication service that is provided by a system

→ Kind (specific) protection to a

system resource.
→ Security Policies.
→ implemented by security mechanisms.

Security Service Purpose

→ Security of Data Processing System and information transfer
→ Using one or more security mechanisms.

Security Services x.800 Style.

1) Authentication
2) Access control
3) Data Confidentiality
4) Data Integrity
5) Non-Repudiation
6) Availability.

Security Mechanisms.

↳ combination of hardware, software and processes.

↳ Mechanisms use security policies.

x.800 mechanism
↳ Specific security mechanisms
(cryptography, digital signature, access control, data integrity, routing control and etc.

↳ Pervasive Security Mechanisms
Trusted functionality, security Labels, security audit trails,

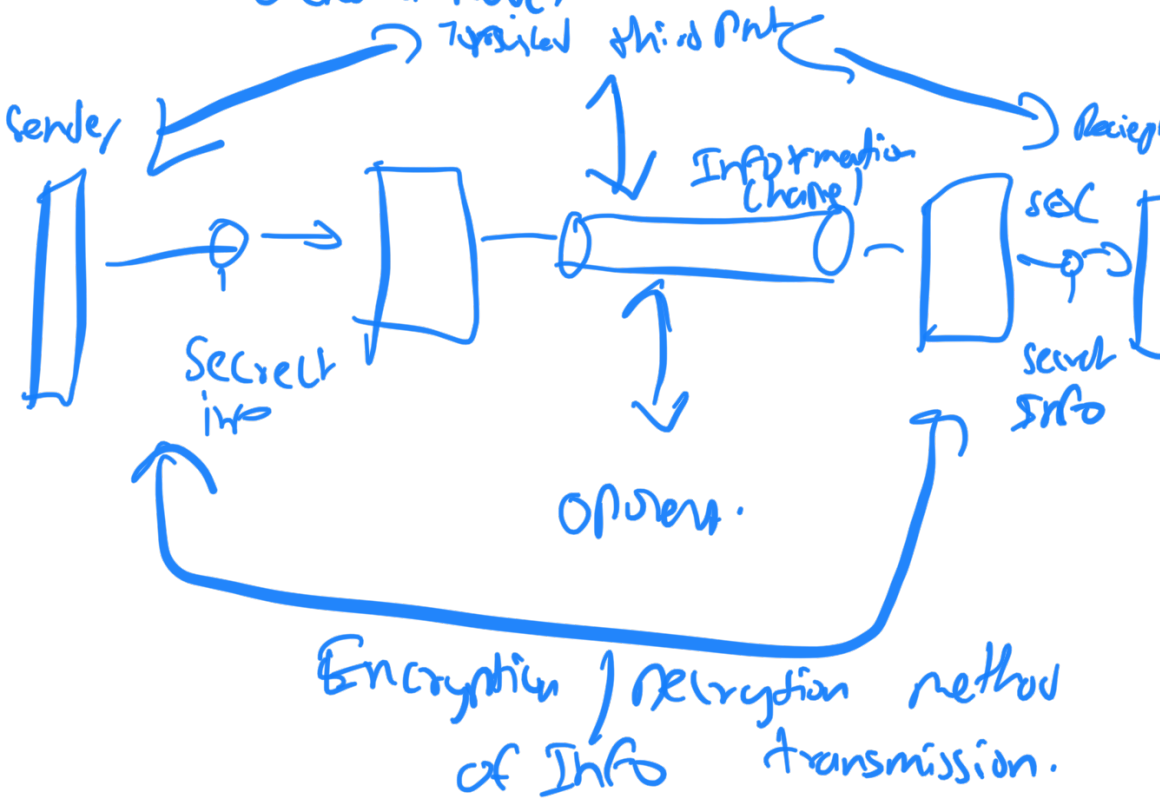
security recovery.

Example Security Mechanisms.

Access control policies being enforced.
- → Credentialling
- → Challenges in DM2
- → Access Auditing.

Network Security Models.

General Model.



Encryption / decryption method of Info transmission.

Motivation for Security Architecture.

→ CCITT → Series of Recommendation to enhance security within Open System Interconnection Architecture.

OSI ENHACED SECURITY

What shall be protected.

a.) Information and Data.
b.) Communication and data processing services
c.) equipment and facilities.

Organizational Threats.

Threats in data communication system include:-

1.) destruction of information
2.) corruption or modification of information
3.) theft, removal or loss of information and/or other resources
4.) disclosure of information; and
5.) interruption of services.

Accidental threats
Intentional → attack
Passive (does not affect system)
Active. → vice versa

Attack
is an action by human, with intent to

violate security.

2 Forms of Passive Attacks.

→ Disclosure
→ Traffic Analysis.
  ↳ information about the message is used in some way.

4 Forms of Active Attack.

1.) Masquerade → Attack on authentication or on Identification.
  ↳ Impersonation.

2.) Replay → A copy of a legitimate message is captured by an opponent and re-transmitted.
  ↳ attack on integrity of the system.

3.) Modification
  ↳ attack on integrity of a system.
  → Content is altered of a legitimate message

4.) Denial of Service.
  ↳ on
  → Opponent prevents authorized users from accessing a system.

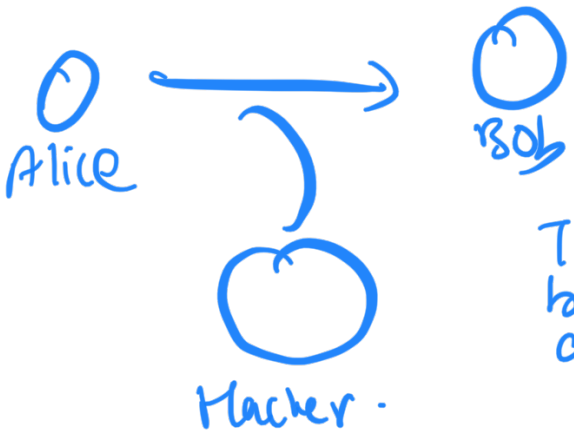
availability of a system.

Security Architecture Attack Model..

1.) Normal Flow of information.

(Active Attack)
Attack: interruption of service.

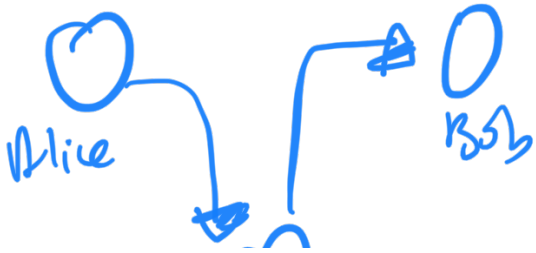
2.) Interception



Panic.

The info arrives but an opponent obtains a copy.

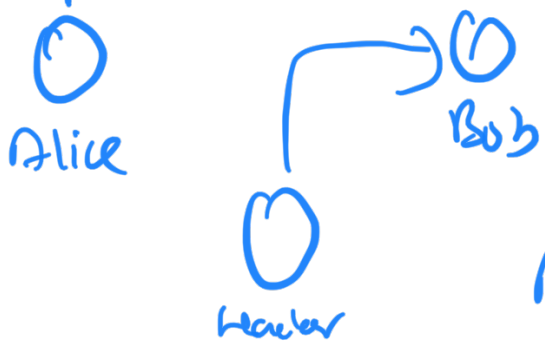
3.) Modification.



The opponent intercepts the original message but forwards a modified version.

Hacker. Active Attack.

4.) Fabrication



An opponent creates a message to have come from a legitimate sore.

Active Attack.

5) Diversion

The message have carries to Bob but the opponent has a copy

Active Attack.

Malware and an Introduction to threat protection

Malware → malicious software is used to disrupt computer or mobile operations and gather sensitive information.

Types of malware:

- Virus
- Worms
- Trojan Horses
- spyware
- Adware
- RAT's
- Rootkit

Ransomware → malware that host with a code that restricts the acces to the computer or the data on it.

Threat Examps

Botnets → set of compromised hosts that enable attacks to exploit those computer resources to mount attacks.

1) Key loggers
2) Logic Bombs
3) APT's

How to protect Against threats?

1) Technical control → AV, IPS, IDS, UTM
   Updates
2) Administrative control → Policies, Training
   Revision and tracking.

The Cyber Kill Chain

1. Reconnaisance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. command & control
7. Actions on objective.

What is social Engineering.
The use of humans for cyber purposes.

SET → Social-Engineer Toolkit
↳ look into this

Phishing & Vishing campaign.

GoPhish → A opensource Phishing Framework.
↳ look into this.
tools to perform phishing Framework.

Vishing → Fake voice to get legitimate information.

Cyberwarfare.

→ Cyber war → link to attack since 2006.

Statistics website around the

Cybercrime Resources

1.) X-Force reports
2.) Personalized reports
3.) Cost of a Data Breach.